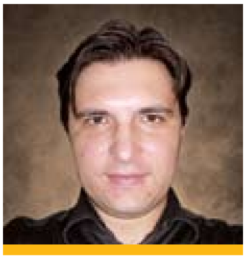
Yonko Yonchev, SAP AG and Peter McNulty, SAP Labs

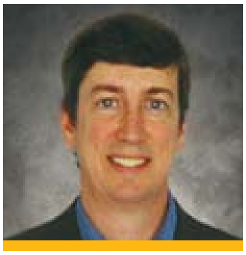
This article appeared in the Oct ▪ Nov ▪ Dec 2009 issue of *SAP Insider* and appears here with permission from the publisher, Wellesley Information Services (WIS), **www.WISpubs.com.**

Enable Governance and Security Across Your Business Processes

4 Key Activities for Security Administrators in an SOA Environment



Yonko Yonchev (yonko.yonchev@sap.com) works for the solution management security department of SAP AG in Walldorf, Germany. Since joining SAP in 2004, Yonko has worked on a variety of security topics regarding access control, single sign-on, Web services security, and Java and portal server security. He has an undergraduate degree in economics and an MBA with a management of information systems concentration from Bentley University.



Peter McNulty (peter.mcnulty@sap.com) is an SAP NetWeaver Director for SAP Labs, focusing on SOA, composite applications, and development tools in ABAP and Java. He has been with SAP since November 1996, starting as an internal ABAP developer for SAP America and eventually managing the same development team prior to joining the SAP NetWeaver Solution Management organization. Peter holds a master's degree in computer information science from La Salle University.

Service-oriented architecture (SOA) promises reuse, flexibility, agility, and ease of integration — all so that IT can keep pace with the speed and collaborative nature of business. But left ungoverned, SOA initiatives may experience setbacks: Symptoms include lack of interoperability, low reuse, duplicate services, security breaches, non-compliance, unpredictable service performance, and outages or even outright failures.

Overcoming these setbacks and realizing the benefits of SOA requires a dedicated governance effort (see sidebar below). And to ensure the integrity of your cross-enterprise business processes and information, that governance effort must be founded on solid security principles.

4 Considerations to Secure Your Business Processes

To secure your business processes within a broader SOA governance effort, you need to consider four main security pillars:

Some Advice on Building an SOA Governance Model

SAP defines SOA governance as the processes, policies, and associated control mechanisms a company establishes to steer the adoption, implementation, and evolution of SOA in line with business needs.

SOA governance depends on several elements: people, policies, processes, methodologies, and tooling — all of which must interact in a holistic manner to maximize the benefits and minimize the risks associated with a service-oriented architecture. What follows are some best practices to create this holistic SOA governance model.

Use your existing ITIL governance platform as a foundation for your SOA governance model. ITIL — which provides a built-in governance framework — is the most widely adopted governance model for enabling IT service management. We recommend building your SOA governance model on top of this framework to help speed up and simplify the SOA implementation process.

Create a center of excellence or governance team that consists of representatives from both IT and business to provide resources and guidance and to oversee the implementation of SOA governance across the organization. This group should be responsible for defining and enforcing SOA-related policies and procedures, as well as ensuring that its policies address both business and technical requirements, adhere to regulatory compliance mandates, and follow company security policies regarding data privacy.

Employ design-time and run-time governance processes to ensure that policies are actually followed and that they continue to govern all phases of the SOA development life cycle — including service identification, creation, reuse, testing, versioning, security, and change. These lifecycle activities are typically grouped as either design-time or run-time governance processes:

- **Design-time activities** focus on applying policies governing the design, development, and deployment of reusable, enterprise-class services and relevant artifacts.
- **Run-time governance** (also known as SOA management) involves monitoring, diagnostics, security, auditing, logging, service-level agreements (SLAs), and policy management and enforcement.

- Access management
- Identity management
- System trust and key management
- Threat and vulnerability management

Let's go through each in more detail and uncover the SAP functionality that supports each area (see sidebar at bottom right for some helpful background).

1. Access Management

As a first step to enabling security across productive business processes, companies must define which users can access applications and impose user identification requirements in the authentication process. For subsequent access requirements and permission assignments, companies should use solutions for identity, risk, and performance management. With these solutions, the assigned authorization and permission profiles are composed from application permission definitions created during the development process with the use of application-integrated, permission-checking APIs.

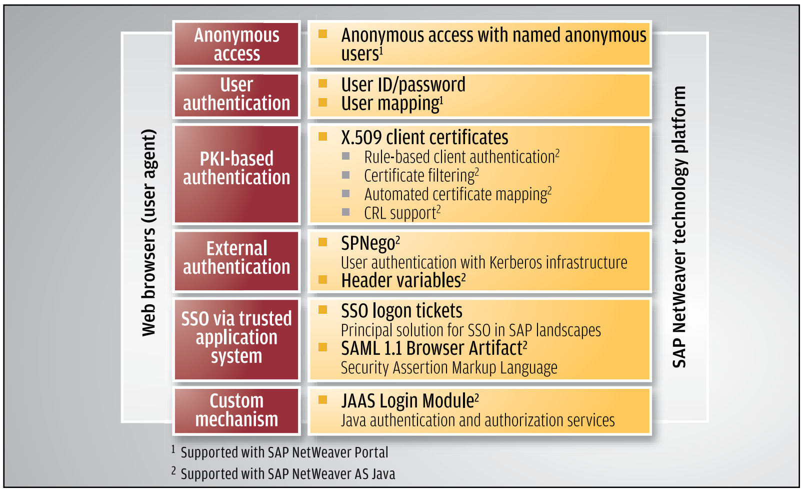
It is important to note that, in terms of access control policies, the SAP user authentication management process and the authorization management process follow separate cycles — SAP authentication is a run-time definition and management activity, while SAP authorization is a development-time definition and run-time management activity. Focusing on user authentication, SAP supports the definition of security policies for user access in SOA applications by:

- Supporting **pluggable handling of various authentication tokens with standards-based integration in common user authentication frameworks.** This integration enables enterprises leveraging SOA applications to employ the user authentication frameworks that best suit their security policy at a relatively low switching cost. The integration options for authentication frameworks (see **Figure 1**) are supported with SAP NetWeaver Application Server (SAP NetWeaver AS) Java and rely on the standardized and commonly used login modules of the JAAS framework. Upcoming SAP NetWeaver releases will also include support for the SAML 2.0 standard.

- Supporting **standardized and secure single sign-on (SSO) solutions** that promote user productivity enablement in distributed service-oriented scenarios in which the users access business applications from both SAP and non-SAP systems. SSO technologies, including SAP logon tickets and SAML 2.0, rely on system certificates to verify the integrity of SSO tokens and transparently enable user access to applications. SAML 2.0 technology specifically enables standardized options for employing single logout and out-of-the-box SSO capabilities for applications with misaligned user identifiers. Both SAML 2.0 and SAP logon tickets allow the use of various mechanisms for initial user authentication and promote secure user productivity enablement through trusted system SSO.

- Providing **identity propagation solutions for managing identity-centered user access to applications** through Web services (WS). Compared to Web applications, which directly interact with end users, service-providing SAP business applications can't directly query a human user for private security credentials. This means that the SAP business

FIGURE 1 ▼ Authentication methods for supporting user interactivity with SAP NetWeaver Web applications



Anonymous access	▪ Anonymous access with named anonymous users[1]
User authentication	▪ User ID/password ▪ User mapping[1]
PKI-based authentication	▪ X.509 client certificates ▪ Rule-based client authentication[2] ▪ Certificate filtering[2] ▪ Automated certificate mapping[2] ▪ CRL support[2]
External authentication	▪ SPNego[2] User authentication with Kerberos infrastructure ▪ Header variables[2]
SSO via trusted application system	▪ SSO logon tickets Principal solution for SSO in SAP landscapes ▪ SAML 1.1 Browser Artifact[2] Security Assertion Markup Language
Custom mechanism	▪ JAAS Login Module[2] Java authentication and authorization services

[1] Supported with SAP NetWeaver Portal

[2] Supported with SAP NetWeaver AS Java

SAP: A Rich History of Supporting Secure Business Processes

Providing secure software solutions that seamlessly support business processes has always been a strategic focus for SAP — SAP has long provided policy enforcement functionality to prevent common security pitfalls and safeguard business information assets. And for security and application governance, the evolution of SAP's applications toward enabling standards-based business process management with SOA applications represented a move away from solutions contained within the "sandbox" of an application server toward solutions encompassing cross-functional application landscapes.

SAP NetWeaver is the technology platform for SAP's business applications and has always included integrated security and identity management functionality — for identity and authorization management, authentication and single sign-on (SSO), front-end user security, and encryption and digital signatures, for example. The comprehensive functionality is based on established and standardized security solutions, which provide flexibility to allow companies to customize the solution for its industry-specific security needs.

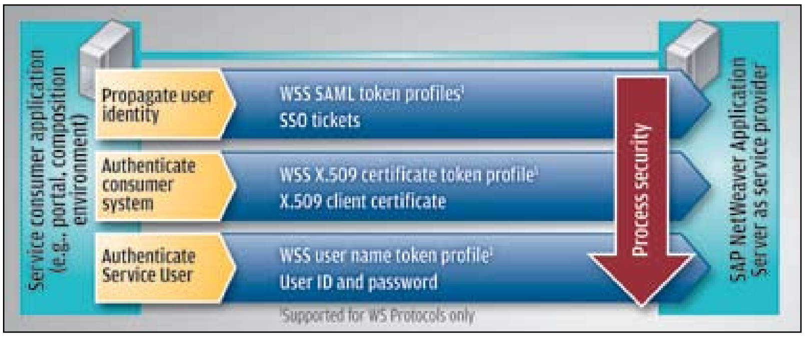

Service consumer application (e.g., portal, composition environment)
Propagate user identity
WSS SAML token profiles¹
SSO tickets
Authenticate consumer system
WSS X.509 certificate token profile¹
X.509 client certificate
Authenticate Service User
WSS user name token profile¹
User ID and password
Process security
SAP NetWeaver Application Server as service provider
¹Supported for WS Protocols only

FIGURE 2 ▲ Authentication methods to support secure access to service applications

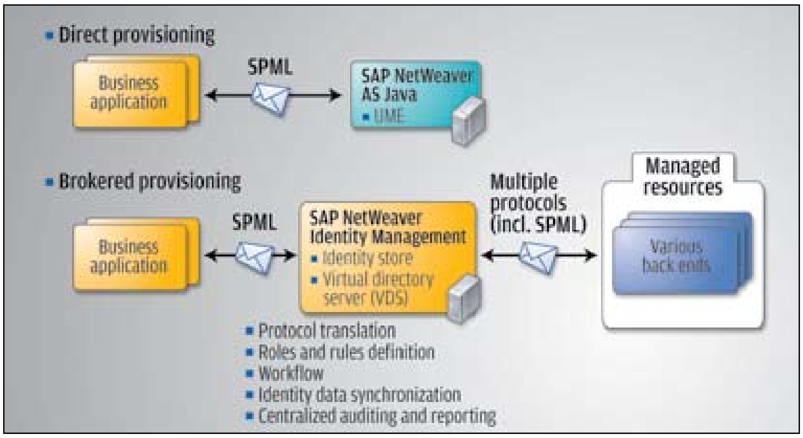


FIGURE 3 ▲ Supply of user identity and authorization information with SPML in SAP NetWeaver BPM

applications that use a Web service must securely propagate the authenticated end user's identity and enable auditability and identity-centered authorization checking within the service provider resources. SAP applications meet this requirement through the deployment of SSO tickets or WS Security (WSS) SAML token profiles (see **Figure 2**).

2. Identity Management

To enable consistent user authorization and identity management across business processes and applications, companies need to have a central, consolidated repository to manage user identities and the various attributes they might hold – including application permission assignments. And remember, one user might need to access resources from numerous business applications. One solution that enables this consolidation is SAP NetWeaver Identity Management (SAP NetWeaver ID Management),[1] which (in conjunction with the applications it is integrated with) enables:

- **External user identity management in dedicated user repositories** – This functionality supports the separation of user management from the application management life cycle by storing user information in a centralized identity store. This information is then made available for applications through standardized protocols, such as LDAP and service provisioning markup language (SPML). SAP NetWeaver Business Process Management (SAP NetWeaver BPM) achieves this separation through the User Management Engine (UME) component of SAP NetWeaver AS Java. The identity store itself can range from a database to an AS ABAP, LDAP directory, or full-blown identity management solution.

- **Externalized end-user authorization assignment and removal** – A key part of identity management is assigning user roles and defining the permissions needed for certain applications. Application developers use standardized SAP authorization concepts to define these permissions. Then, administrators in productive landscapes can group the permissions into roles and user profiles using tools such as SAP NetWeaver ID Management, which only they can access.

- **The supply of user identity information from SAP NetWeaver BPM** – This helps enable comprehensive management processes and user role management. In addition to user provisioning protocols – such as SPML (see **Figure 3**) – identity federation protocols such as SAML 2.0 offer capabilities to optimize identity management activities and enable secure access to information resources using only user attributes, such as line organization roles, functional roles, and project assignments.[2] Thus, upcoming federated identity management capabilities will be key to improving the cost-benefit ratios of identity management solutions.

3. System Trust and Key Management

More and more companies are using cryptographic solutions to secure user access to their business applications. For these companies, knowing how best to manage system trust and key exchanges is critical. SSO allows users to access the multiple applications involved in a business process without having to sign in multiple times, thereby promoting better efficiency.[3]

[1] For more information on SAP NetWeaver Identity Management, see "Identity Management That's Integrated into Your Current Business Processes: Enable Business Process Owners to Manage Access Rights and Roles," a Security Strategies column by Regine Brehm and Jens Koster in the July-September 2009 issue of *SAP Insider* (sapinsider.wispubs.com).

[2] For an overview of SAML 2.0 capabilities, visit www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf.

[3] For more information on SSO, see "How to Future-Proof the Security of Your System Infrastructure in a Service-Enabled World: Apply Tried and True SSO Concepts," a Security Strategies column by Yonko Yonchev in the July-September 2008 issue of *SAP Insider* (sapinsider.wispubs.com).

Securing SSO means setting up cryptography-backed trust relationships between the different applications or their underlying application servers. For SAP applications, these trust relationships and the SSO process itself are made secure with the use of **system key pairs and the import of public key certificates** for the secure identification of trusted SSO-issuing systems.

Keeping track of these trust relationships is critical to efficiently managing the security of the user's SSO access rights and the automated application processes. In automated transactions or when a user accesses a system through SSO, an SAP SSO-issuing system securely signs the SSO token using its private key while counterpart applications use the SAP system's public key to securely verify the SSO token and the user identity information that is submitted with it. SAP supports the associated configuration activities with **key administration and SSO configuration wizards**, which are built into each of SAP's application servers and protected with role-based authorizations. SAP is also planning upcoming solutions that will support key exchanges as part of the initial metadata exchange within a trusted systems setup.

4. Threat and Vulnerability Management

Threat and vulnerability management are multifaceted topics, ranging from preventing lower-level attacks against applications, to securing network layouts, to adopting software quality assurance methodologies. Security protection is always subject to constantly changing risk exposures. And while 100% security is frequently not economically feasible, out-of-the-box SAP applications have solid integrity protection — **SAP's quality assurance processes and security standard requirements**, which all SAP applications must meet throughout the SAP development cycle, mandate this level of security.

To best manage risks across business processes that are running in productive SAP installations and custom applications, you can rely on multiple **threat and vulnerability management functions built into the SAP NetWeaver platform**. These features include virus protection, secure message exchanges for end-to-end security and secure interoperability, built-in output validation in Web Dynpro UI frameworks, options for integration in secured networks, and distributed process auditing. The specific solutions that enable these functions include standards-based solutions — like WSS, XML encryption, XML signatures, and SSO tokens — and are complemented with partner products integrated into the SAP application via certifiable APIs.

Another requirement for compliance and application governance is, of course, auditing. Auditing solutions predominantly rely on a centralized component — like SAP NetWeaver ID Management or SAP's Computing Center Management System (CCMS) — for aggregating local audit records from distributed application processes. CCMS offers a certifiable interface for further audit log aggregation. Please note that, due to limited standardization around the exchange of auditing records, auditing solutions often need to be complemented with proprietary solutions.

Conclusion and Outlook

SOA governance can be a daunting topic, but it is critical to the success of your SOA initiatives. And within an SOA governance plan, we strongly advise a dedicated security effort. We've now armed you with a solid framework of ideas and actions to consider as you secure your business processes and properly govern your SOA activities.

SOA governance can be a daunting topic, but it is critical to the success of your SOA initiatives. And within an SOA governance plan, we strongly advise a dedicated security effort.

SAP is dedicated to providing security solutions to help you ensure the integrity of your business processes. Upcoming releases of SAP NetWeaver will provide additional standards-based security functionality by continuously embracing mature industry standards to enable secure interoperability and boost the return on your investment in software solutions.

For more information about SOA governance and security, please visit **www.sdn.sap.com/irj/sdn/security**.

Additional Resources...

...from SAP insider

- "How to Future-Proof the Security of Your System Infrastructure in a Service-Enabled World: Apply Tried and True SSO Concepts," a Security Strategies column by Yonko Yonchev (*SAP Insider*, July-September 2008, **sapinsider.wispubs.com**)
- The **Administration and Infrastructure 2010** conference in Orlando, Florida, March 23-26, 2010 (**www.sapinsideradmin2010.com**)
- *SAP Securities and Authorizations* by Mario Linkies and Frank Off (SAP PRESS, **www.sap-press.com**)